What is claimed is:

1. A computer program product for efficiently generating pseudo-random bits, the computer program product embodied on one or more computer readable media and comprising:

computer-readable program code means for providing an input value; and

computer-readable program code means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length of the input value is substantially shorter than a length of the generated output sequence.

2. The computer program product according to Claim 1, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

3. The computer program product according to Claim 1, wherein the 1-way function is modular exponentiation modulo a safe prime number.

4. The computer program product according to Claim 3, wherein the input value is used an exponent of the modular exponentiation.

5. The computer program product according to Claim 3, wherein a base of the modular exponentiation is a fixed generator value.

6. The computer program product according to Claim 4, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

7. The computer program product according to Claim 1, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

8. The computer program product according to Claim 1, further comprising:

computer-readable program code means for selecting a subset of bits from the generated output sequence as a next sequential input value, wherein a length of the selected subset is identical to the length of the input value; and

computer-readable program code means for generating a next sequential output sequence of pseudo-random bits using the next sequential input value as input to the 1-way function, wherein a length of the next sequential output sequence is identical to the length of the generated output sequence.

9. The computer program product according to Claim 8, further comprising:

computer-readable program code means for concatenating bits of the generated next sequential output sequence which are not selected by the computer-readable program code means for selecting to the generated output sequence to form a longer output sequence of pseudo-random bits.

10. The computer program product according to Claim 8, wherein the computer-readable program code means for selecting the subset of bits comprises selecting a contiguous group of bits.

11. The computer program product according to Claim 8, wherein the computer-readable program code means for selecting the subset of bits comprises selecting a non-contiguous group of bits.

12. The computer program product according to Claim 8, further comprising computer-readable program code means for using the longer output sequence as input to an encryption operation.

13. A system for efficiently generating pseudo-random bits in a computing environment, comprising:

means for providing an input value; and

means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length of the input value is substantially shorter than a length of the generated output sequence.

14. The system according to Claim 13, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

15. The system according to Claim 13, wherein the 1-way function is modular exponentiation modulo a safe prime number.

16. The system according to Claim 15, wherein the input value is used an exponent of the modular exponentiation.

17. The system according to Claim 15, wherein a base of the modular exponentiation is a fixed generator value.

18. The system according to Claim 16, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

19. The system according to Claim 13, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

20. The system according to Claim 13, further comprising:

means for selecting a subset of bits from the generated output sequence as a next sequential input value, wherein a length of the selected subset is identical to the length of the input value; and

means for generating a next sequential output sequence of pseudo-random bits using the next sequential input value as input to the 1-way function, wherein a length of the next sequential output sequence is identical to the length of the generated output sequence.

21. The system according to Claim 20, further comprising:

means for concatenating bits of the generated next sequential output sequence which are not selected by the means for selecting to the generated output sequence to form a longer output sequence of pseudo-random bits.

22. The system according to Claim 20, wherein the means for selecting the subset of bits comprises selecting a contiguous group of bits.

23. The system according to Claim 20, wherein the means for selecting the subset of bits comprises selecting a non-contiguous group of bits.

24. The system according to Claim 20, further comprising means for using the longer output sequence as input to an encryption operation.

25. A method for efficiently generating pseudo-random bits, comprising the steps of:

providing an input value; and

generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length of the input value is substantially shorter than a length of the generated output sequence.

26. The method according to Claim 25, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

27. The method according to Claim 25, wherein the 1-way function is modular exponentiation modulo a safe prime number.

28. The method according to Claim 27, wherein the input value is used an exponent of the modular exponentiation.

29. The method according to Claim 27, wherein a base of the modular exponentiation is a fixed generator value.

30. The method according to Claim 28, wherein the length of the input value is at least 160 bits and a length of the safe prime number is at least 1024 bits.

31. The method according to Claim 25, wherein the length of the input value is 160 bits and the length of the generated output sequence is 1024 bits.

32. The method according to Claim 25, wherein the length of the input value is at least 160 bits and the length of the generated output sequence is at least 1024 bits.

33. The method according to Claim 25, further comprising the steps of:

selecting a subset of bits from the generated output sequence as a next sequential input value, wherein a length of the selected subset is identical to the length of the input value; and

generating a next sequential output sequence of pseudo-random bits using the next sequential input value as input to the 1-way function, wherein a length of the next sequential output sequence is identical to the length of the generated output sequence.

34. The method according to Claim 33, further comprising the step of concatenating bits of the generated next sequential output sequence which are not selected by the selecting step to the generated output sequence to form a longer output sequence of pseudo-random bits.

35. The method according to Claim 33, wherein the step of selecting the subset of bits comprises selecting a contiguous group of bits.

36. The method according to Claim 33, wherein the step of selecting the subset of bits comprises selecting a non-contiguous group of bits.

37. The method according to Claim 33, further comprising the step of using the longer output sequence as input to an encryption operation.

38. The method according to Claim 25, further comprising the steps of:

repeatedly generating additional output sequences, further comprising the steps of:

selecting a subset of bits from a next prior generated output sequence as a next input value, wherein a length of the selected subset is identical to the length of the input value; and

generating a next output sequence of pseudo-random bits using the next input value as input to the 1-way function, wherein a length of the next output sequence is identical to the length of the generated output sequence; and

concatenating bits of each of the repeatedly generated additional output sequences which are not selected by the selecting step to form a pseudo-random output sequence.

39. An encryption system, comprising:

means for providing an input value;

means for generating an output sequence of pseudo-random bits using the provided input value as input to a 1-way function, wherein a length of the input value is substantially shorter than a length of the generated output sequence; and

means for using bits of the generated output sequence as input to an encryption operation.

40. The encryption system according to Claim 39, wherein the 1-way function is based upon an assumption known as "the discrete logarithm with short exponent" assumption.

41. The encryption system according to Claim 39, wherein the 1-way function is modular exponentiation modulo a safe prime number.

42. The encryption system according to Claim 41, wherein the input value is used an exponent of the modular exponentiation.

43. The encryption system according to Claim 41, wherein a base of the modular exponentiation is a fixed generator value.

44. The encryption system according to Claim 42, wherein the length of the input value is 160 bits and a length of the safe prime number is 1024 bits.

45. The encryption system according to Claim 39, wherein the length of the input value is 160 bits and the length of the generated output sequence is 1024 bits.

46. The encryption system according to Claim 39, further comprising:

means for selecting a subset of bits from the generated output sequence as a next sequential input value, wherein a length of the selected subset is identical to the length of the input value; and

means for generating a next sequential output sequence of pseudo-random bits using the next sequential input value as input to the 1-way function, wherein a length of the next sequential output sequence is identical to the length of the generated output sequence.

47. The encryption system according to Claim 46, further comprising:

means for concatenating bits of the generated next sequential output sequence which are not selected by the means for selecting to the generated output sequence to form a longer output sequence of pseudo-random bits; and

wherein the means for using bits of the generated output sequence as input to the encryption operation further comprises means for using the longer output sequence as the input to the encryption operation.